ISSN: 0976-3104
SPECIAL ISSUE : Computer Science

ARTICLE

A CRYPTOGRAPHICALY IMPOSED DCP-ABE-M SCHEME WITH ATTRIBUTE BASED PROXY RE-ENCRYPTION AND KEYWORD SEARCH IN UNTRUSTED PUBLIC CLOUD

Suraj U Rasal[1], Varsha S Rasal[1], Shraddha T Shelar[2]

[1*]*Computer Engineering Department, Bharati Vidyapeeth University College of Engineering Pune, INDIA*

[1]*Department of Computer Science & Engineering, Nehru College of Engineering & Research Center, Thrissur, Kerala, INDIA*

[2]*Department of Information Technology, DY Patil College of Engineering Akurdi, Pune, INDIA*

ABSTRACT

Encryption on the user data before outsourcing it into the cloud is an inevitable task. Keyword searching is an influential technique which enables the cloud to conduct keyword searching on the encrypted data which allows performing various search operations on re-encrypted data for rapid data retrieval. Most of the existing schemes had focused on single user scenario. The proposed system concentrates on the multiple senders and multiple user scenarios. Here we have merged the concepts of DCP-ABE-M (Decentralized Cipher Policy Attribute Based Encryption with mediator) with ABRKS (Attribute Based proxy Re-encryption with Keyword Search) which enables the option of advance secure re-encryption and keyword searching in unsecure public cloud. The proposed DCP-ABE-M-ABRKS (Decentralized Cipher Policy Attribute Based Encryption with mediator - Attribute Based proxy Re-encryption with Keyword Search) system provides some special features such as: (i). data owner can ask the cloud to conduct keyword search, on his encrypted data by using the user given search token, (ii). Cloud re-encrypts the available cipher text by using a cryptographically enforced DCP-ABE-M technique which contains additional features for data security. Hence, the proposed system is more reliable than the existing systems.

KEY WORDS
Public key Encryption, Proxy Re-encryption, Keyword Search, cloud storage, DCP-ABE, Mediator, OTP.

Received: 16 December 2016
Accepted: 15 January 2016
Published: 15 February 2017

***Corresponding Author**
Email:
surasal@bvucoep.edu.in
Tel.: +918793000079

INTRODUCTION

Eminently, cloud computing is the prominent platform which assemble tremendous computational resources and make them available as a service to varies users. The cloud users can store their data and can enjoy the promising properties of cloud. Predominantly, there are three types of clouds: 1) public cloud: they are owned and operated by companies and provide rapid services to users, 2) private cloud: they are owned and operated by a single organization and provides rapid services for specific authorized user, 3) hybrid cloud: it's a combination of public cloud and private cloud where the users can enjoy the facilities of public cloud also. Public cloud is more reliable, cost saving and elastic in nature than private cloud. Public cloud provides some benefits such as: SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service). Inorder to store the data into the cloud the user must encrypt the data before outsourcing it into the cloud for safeguarding the data privacy.

The most important benefits of using cloud are low maintenance cost, pervasive accessing and storage flexibility etc. But on the other hand, cloud storage faces many troubles against service quality [1][2] and vulnerabilities.

In order to ameliorate the data privacy the existing scheme [4] added public key encryption techniques in cloud storage which allows storing the encoded data in the cloud. That is for safeguarding the data privacy user should encrypt the data before outsourcing it into the cloud and this scheme had given a token to a designated user so that except that user no one will be able to decrypt the data. But in the case of multicasting this scheme fails. In order to solve this problem proxy re-encryption technique is used [3]. In this scheme a semi trusted proxy re-encrypt the cipher text for remaining users. Yanfeng Shi, Jiqiang Liu proposed a scheme Attribute-Based Proxy Re-Encryption with Keyword Search [5] which allows attribute based re-encryption for the user by using keyword search for fast access.

Here we have embedded the DCP-ABE-M [6] public key encryption scheme, key word search technique with proxy re-encryption [5] and applied it on cloud storage for improving security and faster response.

MATERIALS AND METHODS

This chapter shows the summarized features of the most relevant techniques, proxy re-encryption with keyword search, attribute-based encryption, attribute-based encryption with keyword search and attribute-based proxy re-encryption, DCP-ABE, DCP-ABE-M with OTP.

Public key Encryption: ABE

Inorder to avoid the limitations of IBE (Identity Based Encryption) Sahai and waters had proposed a scheme called ABE (Attribute Based Encryption) [7]. In ABE scheme focal power will be responsible for the global initialization of ABE frame work. Focal power or central authority screens the arrangement of all

attributes of various users and then allocate the mystery keys to users based upon their priority. Prominently, the client can decode the encrypted data if and only if there is a match between the tracts which is attached with the cipher text and the user holding qualities. Henceforth, this system can be used as an essential center in the exploration group.

Attribute-based encryption with keyword search

Zheng QJ, Xu SH had proposed the concept of ABK (Attribute Based Keyword search) [8]. Then this work is extended by Sun WH, Yu SC [9] for increasing the data retrieval speed. This scheme allows the data owner to provide some keywords for their encrypted data so that the authorized users can easily access the cipher text by using those keywords.

Attribute-based proxy re-encryption

Boneh et al. had proposed the first PEKS (Public key Encryption Keyword Search) scheme in 2004 [4]. The concept of designated tester (dPEKS) is used in this scheme, which will only allow a designated server to run the test function (dTest). This scheme fails when the sender wants to send the same message to multiple people. Further, this problem is solved in [3] which introduced the concept of proxy re-encryption technique at first time. Proxy re-encryption scheme allows a semi trusted proxy to encrypt a cipher text or already encoded code into another cipher text of same message by using sender's public key and some special information. This concept is further extended in [10][11][12][13]. But the limitation of this scheme is, it requires more accessing time or the users may face more difficulty in accessing of cipher text.

Proxy Re-encryption with keyword search

The drawback of the scheme [14] can be avoided by adding the concept of keyword searching in it. Inorder to solve the problem of previously existing system Shao J, Cao ZF, Liang XH introduced a new scheme Proxy Re-encryption with Keyword Search [15]. This scheme allows the data owner to provide the option of keywords to other users. Then this concept is further extended by Yau WC, Phan RCW in [16][17][18].

Attribute based proxy re-encryption and keyword search

Yanfeng Shi, Jiqiang Liu introduced the concept ABRKS (Attribute Based Proxy Re-encryption with Keyword Search) [5] in which allows the data owner to conduct the keyword search on the re-encrypted data for other users. Here, the privacy of the keyword is also secured. The following [Fig. 1] represents the re-encryption process.

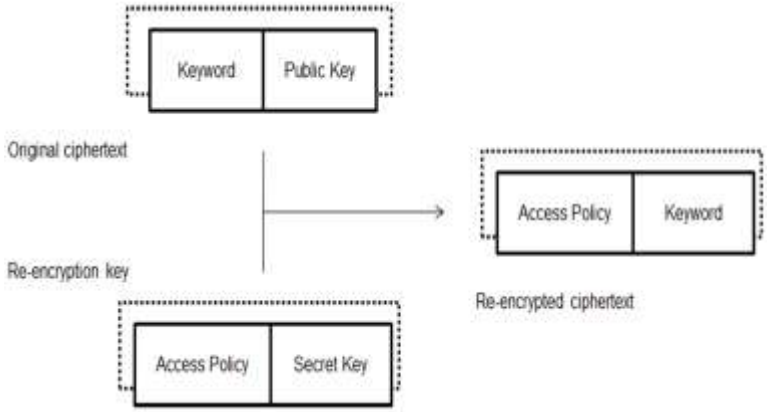

Fig. 1: Enabling the Idea of keyword searching on re-encrypted data

DCP-ABE

Inorder to eliminate the dependency on the focal, Jinguang Han proposed a new scheme called DCP-ABE (Decentralized Cipher text Policy Attribute Based Encryption) scheme [19] which eliminates the drawbacks of existing public key encryption scheme. This system doesn't require a focal for monitoring various components of the system. Multiple independent powers are used in this system which generates secret key without knowing the user attributes, GID and stores the key in a logical manner inorder to secure its privacy. It takes multiple sub secret keys from various powers and they are merged with each other to form the main secret key for a single user. If any power fails then it will be difficult to get the secret key, this is the drawback of DCP-ABE scheme.

DCP-ABE-M

The drawback of the existing scheme can be eliminated through the newly proposed scheme DCP-ABE-M (Decentralized Cipher text Policy Attribute Based Encryption with Mediator) [6]. In this scheme multiple independent powers and mediators are used which are based upon specific attributes. The system allocates a single mediator and power for a single user, who generates secret key for the user based upon the user attributes. The secret key will be split and stored differently in mediator and in power. So that the failure of any component will not affect the entire system.

Table 1: Survey on the existing schemes and its solution

Scheme	Proxy re-encryption	Keyword Search	Access Control	Accessing Speed
PRES [15-18]	✓	✓	x	x
ABE [7]	x	x	✓	x
ABKS [8-9]	x	✓	✓	✓
ABPRE [10-14]	✓	x	✓	x
ABRKS [5]	✓	✓	✓	✓
DCP-ABE [19]	x	x	✓	x
DCP-ABE-M [6]	x	x	✓	x
Proposed system	✓	✓	✓	✓

RESULTS

In the proposed system we have integrated the concept of DCP-ABE-M with proxy re-encryption and keyword searching which enables fast and secure data sharing in cloud. There are 4 factors which plays an important role in this system.

- Focal
- Data owner
- Authorized users
- Cloud

Focal is the central power of the system, which is accountable for the key distribution. When the data owner wishes to outsource his data into the cloud, subsequently the system performs various types of encryption on the data for securing its privacy. In this system data is encrypted two times before storing it in to the cloud. Following [Fig. 2] represents the architecture of the proposed system.

Primary encryption

Before outsourcing of data into the cloud, data owner attach some keywords with data file inorder to get the facility of keyword searching. ABE (Attribute Based Encryption) is used here for primary encryption of data. ABE utilizes the attribute set of user for secret key generation. Here U_A indicates user attribute set, A_n specifies user attribute, S_{K1} represents secret key for first encryption, D_F defines data file, K_I specifies keyword index and E_1 specifies single encrypted file or cipher text.

$U_A = \{A_1, A_2, A_3 \ldots\ldots\ldots A_n\}$
$U_A \rightarrow S_{K1}$
$S_{K1} (D_F + K_I) \rightarrow E_1$
$(S_{K1}.D_F) + (S_{K1}. K_I) \rightarrow E_1$

Here P_E indicates primary encryption,

$P_E \rightarrow D_F + K_I$
$\rightarrow E_1 (D_F + K_I)$
$\rightarrow (E_1.D_F) + (E_1. K_I)$

Subsequently, the encrypted data file is outsourced into the cloud for storage. Cloud is operated by using a semi trusted proxy server. Then the data owner sends a request for keyword search to proxy based upon available token and data. Again data owner sends a request of re-encryption to proxy. Inorder to search

over the re-encrypted data a keyword is given to proxy. By using this keyword, data owner can search on the re-encrypted data for its future retrieval.
Server sends the newly arrived encrypted data file into token recognizer for authentication and verification of token. T_R checks the token and data for verification of user type.

$U_T = E\ K_I$
$T_R \rightarrow \quad U_T \in A_U$
A_U = {Set of authorized user tokens}
If $U_T \in A_U \rightarrow$ authorized user data
Else $U_T \quad A_U \rightarrow$ unauthorized user data

Where, U_T is the user token, $E\ K_I$ defines encrypted keyword index, T_R represents token reorganizer and A_U is the authorized user token set. Here, if newly arrived user token U_T is an element of authorized user token set then that specific user is an authorized or identified user else the user is a fake user. The following flow chart [Fig. 3] represents the processing of this proposed system.

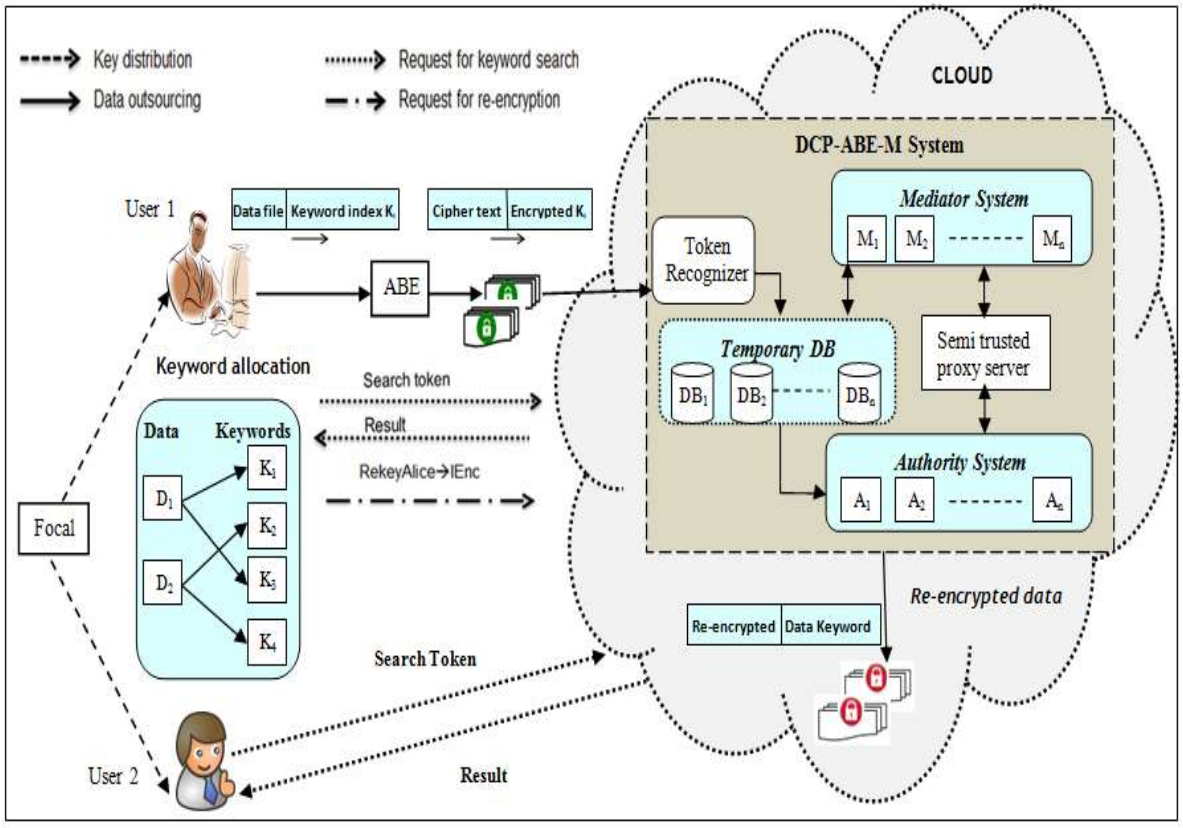

Fig. 2: Architecture of DCP-ABE-M-ABRKS system.

Secondary encryption

The proposed system has used DCP-ABE-M technique for performing secondary encryption. DCP-ABE-M system mainly contains 3 components.

- Mediator system
- Authority system
- Temporary data base

Mediator system contains multiple independent mediators who verifies and checks the attributes of incoming token for the further redirection toward specific authority. Each mediator and authority is based upon some special attributes or characteristics and they takes user data based upon the user attributes or character which matches with their own character. The main purpose of mediator is for storing the half secret key for the security improvement of system.

Here, the token reorganizer verifies the incoming token and stores the data into a specific temporary DB. For each and every user, our system builds a temporary DB and deletes the DB after secret key creation.

Then based upon user type or attribute, our system directs the user towards the mediator which have some matching characteristics of user. For example: business related user is directed towards a mediator who is based upon business attribute. Mediator again verifies all the user details by extracting it from temp DB of that user and direct towards matching authority.

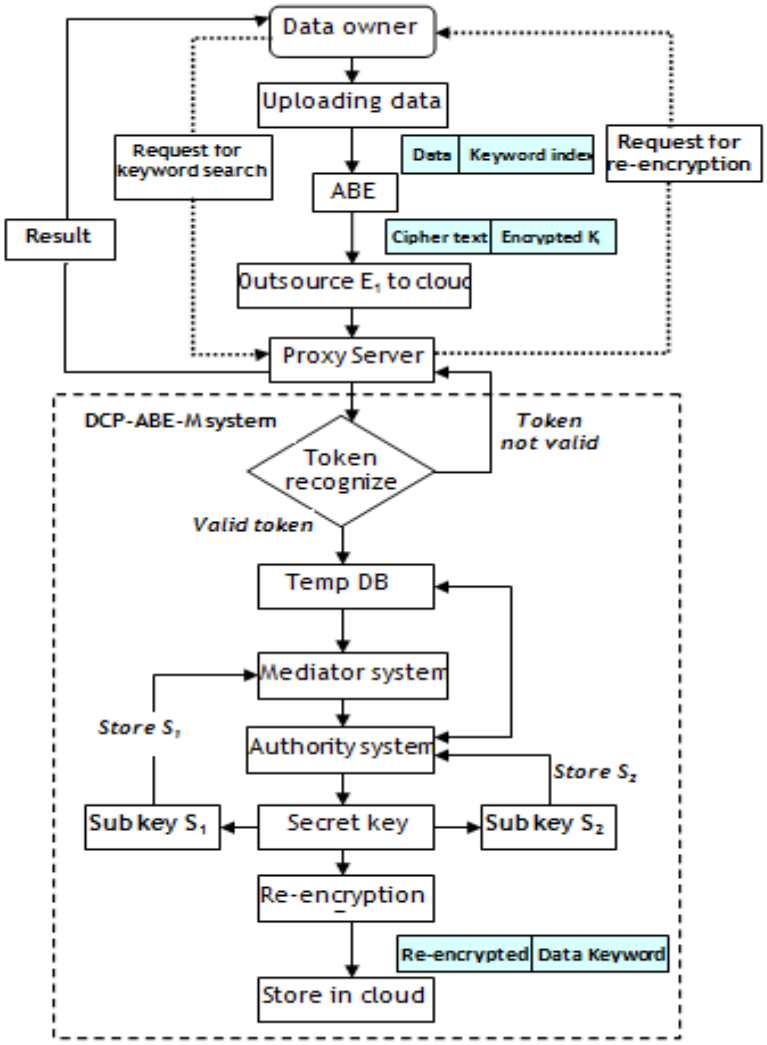

Fig. 3: Flow chart for DCP-ABE-M-ABPKS system processing.

Authority system contains number of independent authorities who generates secret keys for the user. By extracting the details form temp DB, authority generates the secret key for the user which is used for the data encryption.

$S_E \longrightarrow [P_E]\ S_{K2}$ ..... (1)
$S_{K2} = U_A + U_T + D_A$

Here, S_E indicates secondary encryption and S_{K2}defines second secret key used for the re encryption. S_{K2} is generated by using user attributes U_A, user token U_T and data attribute D_A.

$U_A = \{U_1, U_2, U_3 \ldots\ldots U_n\}$
$U_T = E_1 K_I$
$D_A = \{D_1, D_2, D_3 \ldots\ldots D_n\}$
$U_A \cup U_T \cup D_A = S_{K2}$
We have
$P_E \longrightarrow (E_1. D_F + E_1. K_I)$ ..... (2)
Use (2) in (1) this in S_E
$S_E \longrightarrow (E_1. D_F + E_1. K_I)\ S_{K2}$
$S_E \longrightarrow (E_1. D_F. S_{K2} + E_1. K_I. S_{K2})$
$S_E \longrightarrow E_2$

E_2 specifies re-encrypted data file. By using the secret key S_{K2} , E_1 is re-encrypted. After the encryption data is stored along with keyword by applying some access policy and then subsequently the temp DB is deleted. Prominently, the available secret key S_{K2} is divided into two parts and one part is stored in the mediator and another part is stored in the authority.
When any user tries to access data, focal check the user attributes for authentication and then if the user is an authorized user then the system allows him to access the data and provides specific keyword.

CONCLUSION

The proposed scheme is an integration of technologies in the area of cryptography. The concept of DCP-ABE-M-ABRKS technique can be used in the unsecure public cloud which provides the features like: secure re-encryption, keyword searching facility on encrypted data, securing the privacy of the keyword. Hence our system is more secure and faster in data retrieval than the other existing schemes.

CONFLICT OF INTEREST
There is no any form of conflict of interest

ACKNOWLEDGEMENTS
None

FINANCIAL DISCLOSURE
None

REFERENCES

[1] Ding S, Yang SL, Zhang YT, Liang CY, Xia CY. [2014] Combining qos prediction and customer satisfaction estimation to solve cloud service trustworthiness evaluation problems. Knowl-Based Syst 56: 216–225.

[2] Ding S, Xia CY, Zhou KL, Yang SL, Shang JS. [2014] Decision support for personalized cloud service selection through multi-attribute trustworthiness evaluation. PloS one 9(6): e97762.

[3] Blaze M, Bleumer G., Strauss M. [1998] Divertible protocols and atomic proxy cryptography. *In: Nyberg*, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 127–144. Springer, Heidelberg.

[4] Boneh D, Crescenzo GD, Ostrovsky R, Persiano G. [2004] Public key encryption with keyword search. *In: Cachin C, Camenisch, J.L.* (eds.) EUROCRYPT 2004. LNCS, vol. 3027:. 506–522. Springer, Heidelberg.

[5] Yanfeng Shi, Jiqiang Liu, Zhen Han. [2014] Attribute-Based Proxy Re-Encryption with Keyword Search. PloS one 9(12): e116325.

[6] Varsha Thanaji Mulik, Shinu A, Suraj Rasal. [2016] Privacy Preserving Through Mediator in Decentralized Ciphertext policy Attribute Based Encryption, IJRET: International Journal of Research in Engineering and Technology, 05 (06) | Jun.

[7] Sahai and B. Waters. [2005] Fuzzy identity-based encryption, in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 3494. Heidelberg, Germany: Springer-Verlag, pp. 457–473.

[8] Zheng QJ, Xu SH, Ateniese G. [2014] VABKS: verifiable attribute-based keyword search over outsourced encrypted data. In: 2014 IEEE Conference on Computer Communications, INFOCOM 2014, Toronto, Canada, April 27 - May 2. pp. 522–530.

[9] Sun WH, Yu SC, Lou WJ, Hou YT, Li H. [2014] Protecting your right: Attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud. In: 2014 IEEE Conference on Computer Communications, INFOCOM 2014, Toronto, Canada, April 27 - May 2, 2014. pp. 226–234.

[10] Li KY, Wang JF, Zhang YH, Ma H . [2014] Key policy attribute-based proxy re-encryption and rcca secure scheme. Journal of Internet Services and Information Security (JISIS) 4: 70–82.

[11] Liang XH, Cao ZF, Lin H, Shao J. [2009] Attribute based proxy re-encryption with delegating Capabilities. In: Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. ACM, pp. 276–286.

[12] Luo S, Hu JB, Chen Z. [2010] Ciphertext policy attribute-based proxy re-encryption. *In: Information and Communications* Security, Springer. pp. 401–415.

[13] Mizuno T, Doi H. [2011] Hybrid proxy re-encryption scheme for attribute-based encryption. *In: Information Security and Cryptology*. Springer, pp. 288–302.

[14] Guo SQ, Zeng YP, Wei J, Xu QL. [2008] Attribute-based re-encryption scheme in the standard model. Wuhan University Journal of Natural Sciences 13: 621–625.

[15] Shao J, Cao ZF, Liang XH, Lin H. [2010] Proxy re-encryption with keyword search. Information Sciences 180: 2576–2587.

[16] Yau WC, Phan RCW, Heng SH, Goi BM. [2010], Proxy re-encryption with keyword search: new definitions and algorithms. *In: Security Technology, Disaster Recovery and Business Continuity,* Springer. pp. 149–160.

[17] Fang LM, Susilo W, Ge CP, Wang JD. [2012] Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search. Theoretical Computer Science 462: 39–58.

[18] Wang XA, Huang XY, Yang XY, Liu LF, Wu XG. [2012] Further observation on proxy re-encryption with keyword search. Journal of Systems and Software 85: 643–654.

[19] Jinguang han, willy susilo, yi mu, jianying zhou, Man ho allen au. [2015] improving privacy and security in decentralized ciphertext-policy attribute-based encryption, ieee transactions on *information forensics and security*. 10(3) (1):665-678.